

WHAT IS CLAIMED IS:

1. A method of communicating with an element within an enterprise network, comprising:

5 at a first client, encapsulating a first point-to-point protocol signal within a network address request header; and

communicating the network address request encapsulated signal toward a tunneling server.

10 2. The method of Claim 1, wherein the network address request header comprises a Dynamic Host Configuration Protocol DISCOVER header or a Bootstrap Protocol REQUEST header.

15 3. The method of Claim 1, wherein communicating the network address request encapsulated signal toward a tunneling server comprises communicating the signal toward a router configured to relay network address requests to the tunneling server without referencing a routing table
20 indexed by data channel addresses.

4. The method of Claim 3, wherein the first point-to-point protocol signal comprises a control channel address of a second client, the control channel address
25 being different from any data channel address recognized by the router.

5. The method of Claim 1, wherein the first point-to-point protocol signal comprises a payload including
30 information to be applied to an application residing at a second client.

6. The method of Claim 5, wherein the application residing at the second client comprises a maintenance application operable to diagnose operational characteristics of the second client.

5

7. The method of Claim 1, wherein the first point-to-point protocol signal comprises a payload including at least a portion of an application to be installed on a second client.

10

8. The method of Claim 1, further comprising encapsulating the first point-to-point protocol signal within a tunneling header prior to encapsulating the first point-to-point protocol signal within the network address request header, the tunneling header operable to facilitate a tunneling session between the first client and the tunneling server.

15

9. The method of Claim 8, wherein the tunneling header comprises a tunneling header selected from the group consisting of a Layer Two Tunneling Protocol (L2TP) header, a Point-to-Point Tunneling Protocol (PPTP), or a Layer Two Forwarding (L2F) header.

20

10. The method of Claim 1, further comprising receiving a network address response encapsulated signal from the tunneling server, the network address response encapsulated signal comprising a second point-to-point protocol signal responsive to the first point-to-point protocol signal and encapsulated within a network address response header.

25

30

11. The method of Claim 1, wherein the network address response header comprises a Dynamic Host Configuration Protocol OFFER header or a Bootstrap Protocol RESPONSE header.

12. A computer readable medium operable to execute the following steps on a processor of a computer:

at a first client, encapsulating a first point-to-point protocol signal within a network address request header; and

communicating the network address request encapsulated signal toward a tunneling server.

13. The computer readable medium of Claim 12, wherein communicating the network address request encapsulated signal toward a tunneling server comprises communicating the signal toward a router configured to relay network address requests to the tunneling server without referencing a routing table indexed by data channel addresses.

14. The computer readable medium of Claim 13, wherein the first point-to-point protocol signal comprises a control channel address of a second client, the control channel address being different from any data channel address recognized by the router.

15. The computer readable medium of Claim 12, wherein the first point-to-point protocol signal comprises a payload including information to be applied to an application residing at a second client.

16. The computer readable medium of Claim 12, wherein the first point-to-point protocol signal comprises a payload including at least a portion of an application to be installed on a second client.

5 17. The computer readable medium of Claim 12, further comprising encapsulating the first point-to-point protocol signal within a tunneling header prior to encapsulating the first point-to-point protocol signal within the network address request header, the tunneling header operable to facilitate a tunneling session between the first client and the tunneling server.

10 18. The computer readable medium of Claim 12, further comprising receiving a network address response encapsulated signal from the tunneling server, the network address response encapsulated signal comprising a second point-to-point protocol signal responsive to the first point-to-point protocol signal and encapsulated within a
15 network address response header.

19. A method of tunneling in an enterprise network comprising a plurality of clients coupled to a tunneling server by at least one router, the method comprising:

at a first client, generating point-to-point protocol
5 signal;

encapsulating the point-to-point protocol signal
within a network address request header;

communicating the network address request encapsulated
tunneling signal toward a tunneling server operable to
10 identify and remove the network address request header, to
encapsulate the point-to-point protocol signal within a
network address response header, and to communicate the
network address response encapsulated signal toward a
second client.

20. The method of Claim 19, communicating the network
address request encapsulated tunneling signal toward a
tunneling server comprises communicating the signal toward
a router operable to relay the signal toward the tunneling
20 server without referencing a routing table indexed by data
channel addresses.

21. The method of Claim 20, wherein the point-to-
point protocol signal comprises a control channel address
25 of a second client, the control channel address being
different from any data channel address recognized by any
router coupled to the tunneling server.

22. The method of Claim 19, further comprising
30 encapsulating the point-to-point protocol signal within a
tunneling header prior to encapsulating the point-to-point
protocol signal within the network address request header,
the tunneling header operable to facilitate a tunneling
session between the first client and the tunneling server.

23. The method of Claim 19, further comprising receiving a response from the second client, the response forwarded from the tunneling server and comprising a point-to-point protocol signal encapsulated within a network address response header.

5

10

020533.0340

24. In an enterprise network comprising at least one client coupled to a tunneling server by a router having a routing table indexed by data channel addresses, a first client comprising:

5 a protocol stack operable to generate a first point-to-point protocol signal; and

 a tunneling module operable to encapsulate the first point-to-point encapsulated signal within a network address request header;

10 wherein the first client is operable to communicate the network address request encapsulated signal toward the router for forwarding to the tunneling server without reference to the routing table.

15 25. The first client of Claim 24, wherein the network address request header comprises a Dynamic Host Configuration Protocol DISCOVER header or a Bootstrap Protocol REQUEST header.

20 26. The first client of Claim 24, wherein the network address request encapsulated signal comprises a tunneling header encapsulating the first point-to-point signal, the tunneling header operable to facilitate a tunneling session between the first client and the tunneling server.

25 27. The first client of Claim 26, wherein the tunneling header comprises a tunneling header selected from the group consisting of a Layer Two Tunneling Protocol (L2TP) header, a Point-to-Point Tunneling Protocol (PPTP),
30 or a Layer Two Forwarding (L2F) header.

28. The first client of Claim 24, wherein the first point-to-point protocol signal comprises:

an identification of a second client coupled to the tunneling server; and

5 information to be applied to an application residing at the second client.

29. The first client of Claim 28, wherein the identification of the second client comprises a control
10 channel address of the second client, the control channel address being distinct from any data channel address used to index a routing table accessible to the router.

30. The first client of Claim 28, wherein information
15 comprises information to be applied to a maintenance application residing at the second client and operable to diagnose operational characteristics of the second client.

31. The first client of Claim 24, wherein the
20 tunneling module is operable to receive a point-to-point protocol signal encapsulated within a network address response header, the network address response encapsulated signal having been relayed from the tunneling server through the router without reference to a routing table
25 indexed by data channels.

32. The first client of Claim 31, wherein the network address response header comprises a DHCP OFFER header or a Bootstrap Protocol RESPONSE header.

33. In an enterprise network, a client having an enterprise protocol stack operable to process signals received from a data channel and associated with a data channel address, the client comprising:

5 a tunneling module operable to receive a first point-to-point protocol signal encapsulated within a network address response header and to remove the network address response header to expose the first point-to-point protocol signal; and

10 a private protocol stack operable to receive the first point-to-point protocol signal from the tunneling module and to communicate at least a portion of a payload of the first point-to-point protocol signal to a socket layer coupled to an application residing at the client.

15 34. The client of Claim 33, wherein the network address response header comprises a Dynamic Host Configuration Protocol OFFER header or a Bootstrap Protocol RESPONSE header.

20 35. The client of Claim 33, wherein the application comprises a maintenance application operable to diagnose operational characteristics of the second client.

25 36. The client of Claim 33, wherein the application comprises an application operable to process the at least a portion of the payload and to generate an output to be communicated toward another network element.

30

37. The client of Claim 33, wherein:

the private protocol stack is operable to generate a second point-to-point protocol signal comprising a payload carrying at least a portion of the output; and

5 wherein the tunneling module is operable to encapsulate the second point-to-point signal within a network address request header and communicate the network address request encapsulated signal to a router for relaying toward a destination network element without
10 reference to a routing table indexed by data channel addresses.

38. The client of Claim 37, wherein the network address request header comprises a Dynamic Host
15 Configuration Protocol DISCOVER header or a Bootstrap Protocol REQUEST header.

39. The client of Claim 33, wherein the first point-to-point protocol signal is encapsulated within a tunneling
20 header and further encapsulated within the network address response header, and wherein the tunneling module is operable to process the tunneling header to maintain a tunneling session between the client and a tunneling server.

25 40. The client of Claim 39, wherein the tunneling header comprises a tunneling header selected from the group consisting of a Layer Two Tunneling Protocol (L2TP) header, a Point-to-Point Tunneling Protocol (PPTP), or a Layer Two
30 Forwarding (L2F) header.